UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,001	12/02/2003	Fangguo Zhang	ZHAN3005/EM	3166

23364 7590 12/19/2006

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA, VA 22314

EXAMINER	
LE, CANH	
ART UNIT	PAPER NUMBER
2112	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/19/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/725,001	ZHANG ET AL.	
	Examiner	Art Unit	
	Canh Le	2112	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☒ Claim(s) *1,6, 5, and 10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

The disclosure is objected to because of the following informalities: Parings is misspelled in the title "APPARATUS AND METHOD FOR GENERATING AND VERIFYING ID-BASED BLIND SIGNATURE BY USING BILINEAR ***PARINGS***". It should be "APPARATUS AND METHOD FOR GENERATING AND VERIFYING ID-BASED BLIND SIGNATURE BY USING BILINEAR ***PAIRINGS***". Also, Parings is misspelled in the abstract, paragraph [0001], paragraph [0006], paragraph [0009], paragraph [0015], paragraph [0021], and paragraph [0041]. Appropriate correction is required.

The disclosure is objected to because of the following informalities: In paragraph [0034], the verification of the signature is justified by the following equations:

$$e(V',P)= e(\alpha V,P)$$

$$= e(U',+ H_1(m,U')Q_{ID}, P_{pub})$$

The comma after U' should be removed. It should be

$$e(V',P)= e(\alpha V,P)$$

$$= e(U' + H_1(m,U')Q_{ID}, P_{pub})$$

Appropriate correction is required.

Claim Objections

Claims 1 and 6 are objected to because of the following informalities: Parings is misspelled in claims 1 and claim 6. Appropriate correction is required.

Claims 5 and 10 are objected to because of the following informalities: The following equations:

$$e(V',P)= e(\alpha V,P)$$

$$= e(U',+ H_1(m,U')Q_{ID}, P_{pub})$$

The comma after U' should be removed. It should be

$$e(V',P)= e(\alpha V,P)$$

$$= e(U' + H_1(m,U')Q_{ID}, P_{pub})$$

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 and 6 are rejected under 35 U.S.C. 102 (e) as being anticipated by Boneh et al (US 7,113,594 B2).

Claims 1 and 6

As per claims 1 and 6, Boneh discloses a system/method for identity-based encryption and related cryptographic techniques, comprising the steps of:

generating system parameters, selecting a master key, and then disclosing the system parameters by a trust authority (Abstract; Figures 1-3, 5-12; Columns 1-10, 12-16, 21-36; Column 37, lines 1-11);

generating a private key by using a signer's identity and the master key, and then

transferring the private key to the signer through a secure channel by the trust authority (Abstract; Figures 1-3, 5-12; Columns 1-10, 12-16, 21-36; Column 37, lines 1-11);

receiving and storing the system parameters by a user and receiving and storing the system parameters and the private key by the signer (Abstract; Figures 1-3, 5-12; 1-10, 12-16, 21-36; Column 37, lines 1-11);

computing a commitment by using at least one of the system parameters, and then sending the commitment to the user by the signer (Abstract; Figures 1-3, 5-12; Columns 1-10, 12-16, 21-36; Column 37, lines 1-11);

blinding a message by using the commitment and a public key based on the signer's identity, and then sending the blinding message to the signer by the user (Abstract; Figures 1-3, 5-12; Columns 1-10, 12-16, 21-36; Column 37, lines 1-11);

signing the blinding message by using the private key, and then sending the signed message to the user by the signer (Abstract; Figures 1-3, 5-12; Columns 1-10, 12-16, 21-36; Column 37, lines 1-11);

unblinding the signed message by the user; and verifying the signature by the user (Abstract; Figures 1-3, 5-12; 1-10, 12-16, 21-36; Column 37, lines 1-11).

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-10 are rejected under 35 U.S.C. 102(a) as being anticipated by Fangguo Zhang and Kwangjo Kim (Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings, Publisher Springer Berlin/Heidelberg, ISSN 0302-9743, Volume 2727/2003, Book Information Security and Privacy, 2003, ISBN 978-3-540-40515-3, Pages 312-323).

Claim 1

Zhang and Kim disclose a method for generating and verifying an ID-based blind signature by using bilinear parings, the method comprising the steps of:

generating system parameters, selecting a master key, and then disclosing the system parameters by a trust authority (Page 315, section 3.2, lines 12-17; Page 314, section 2, lines 10-14); The center publishes system parameters params = $\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$. A Trust Authority (TA) is equivalent to a Key Generation Center (KGC). The KGC keeps s as a master key

generating a private key by using a signer's identity and the master key, and then transferring the private key to the signer through a secure channel by the trust authority (Page 315, section 3.2, lines 15-20; Page 316, lines 6-11; Page 314, section 2, lines 10-14); A user submits his/her identity information ID to the Key Generation Center (KGC). The KGC computes the user's public key as $Q_{ID} = H_2(ID)$, and returns private key $S_{ID} = sQ_{ID}$. KGC keeps s is a master key. The Trust Authority (TA) is equivalent to the Key Generation Center (KGC).

receiving and storing the system parameters by a user and receiving and storing the system parameters and the private key by the signer (Page 316, lines 7-11); The KGC publishes system parameters params = $\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$. A private key is S_{ID}, where $S_{ID} = sQ_{ID}$.

computing a commitment by using at least one of the system parameters, and then sending the commitment to the user by the signer (Page 316, line 28); Computes $U = rQ_{ID}$, where $Q_{ID} = H_2(ID)$. H_2 is one of the system parameters params = $\{G_1, G_2, e, q, P, P_{pub}, H_1$ and $H_2\}$.

blinding a message by using the commitment and a public key based on the signer's identity, and then sending the blinded message to the signer by the user (Page 316, lines 30-32);

signing the blinded message by using the private key, and then sending the signed message to the user by the signer (Page 316, line 33);

unblinding the signed message by the user (Page 316, line 34); and

verifying the signature by the user (Page 317, lines 1-3),

wherein the system parameters include G_1, G_2, e, q, P, P_{pub}, H_1 and H_2, where G_1 is a cyclic additive group whose order is a prime q, G_2 is a cyclic multiplicative group of the same order q, e is a bilinear paring defined by e: $G_1 x G_1 \rightarrow G_2$, P is a generator of G_1, P_{pub} is a trust authority's public key having relationship of $P_{pub}=s.P$, where s is the master key, and H_1 and H_2 are hash functions, respectively, described by H_1: $\{0,1\}^* \rightarrow Z_q^*$ and H_2: $\{0,1\}^* \rightarrow G_1$, where Z_q^* is a cyclic multiplicative group (Page 315, section 3.2, lines 12-17; Page 316, lines 6-8),

wherein the public key Q_{ID} is described by $Q_{ID} = H_2(ID)$, where ID is the signer's identity, and the private key S_{ID} is described by $S_{ID} = sQ_{ID}$ (Page 315, section 3.2, lines 12-17; Page 316, lines 10-11), and

wherein the commitment U is described by $U = r. Q_{ID}$, where r is a random number the signer chooses (Page 316, lines 28-29).

Claim 2

Zhang and Kim disclose the method of claim 1, wherein the blinded message h is described by $h=\alpha^{-1}H_1(m, U')+\beta$, where m is a message to be sent, U' is described by $U'=\alpha U+ \alpha \beta Q_{ID}$ and α and β are blinding factors belonging to Z_q^* (Page 316, lines 28-32).

Claim 3

Zhang and Kim disclose the method of claim 2, wherein the signed message is described by $V=(r+h)S_{ID}$ (Page 316, line 33).

Claim 4

Zhang and Kim disclose the method of claim 3, wherein the step of unblinding is performed by using formula $V' = \alpha V$ (Page 316, line 34).

Claim 5

Zhang and Kim disclose the method of claim 4, wherein the step of verifying is preformed by using following equations: $e(V',P) = e(U', +H_1(m,U')Q_{ID}, P_{pub})$ (Page 317, line 3, lines 9-15).

Claim 6

Zhang and Kim disclose an apparatus for generating and verifying an ID-based blind signature by using bilinear parings, the apparatus comprising:

means for generating system parameters, selecting a master key, and then disclosing the system parameters by a trust authority (Page 315, section 3.2, lines 12-17; Page 314, section 2, lines 10-14);

means for generating a private key by using a signer's identity and the master key, and then transferring the private key to the signer through a secure channel by the trust authority (Page 315, section 3.2, lines 15-20; Page 316, lines 6-11; Page 314, section 2, lines 10-14);

means for receiving and storing the system parameters by a user and receiving and storing the system parameters and the private key by the signer (Page 316, lines 7-11);

means for computing a commitment by using at least one of the system parameters, and then sending the commitment to the user by the signer (Page 316, line 28);

means for blinding a message by using the commitment and a public key based on the signer's identity, and then sending the blinded message to the signer by the user (Page 316, lines 30-32);

means for signing the blinded message by using the private key, and then sending the signed message to the user by the signer (Page 316, line 33);

means for unblinding the signed message by the user; and means for verifying the signature by the user (Page 316, line 34),

wherein the system parameters include G_1, G_2, e, q, P, P_{pub}, H_1 and H_2, where G_1 is a cyclic additive group whose order is a prime q, G_2 is a cyclic multiplicative group of the same order q, e is a bilinear paring defined by e: $G_1 x G_1 \rightarrow G_2$, P is a generator of G_1, P_{pub} is a trust authority's public key having relationship of $P_{pub}=s.P$, where s is the master key, and H_1 and H_2 are hash functions, respectively, described by H_1: $\{0,1\}^* \rightarrow Z_q^*$ and H_2: $\{0,1\}^* \rightarrow G_1$, where Z_q^* is a cyclic multiplicative group (Page 315, section 3.2, lines 12-17; Page 316, lines 6-8),

wherein the public key Q_{ID} is described by $Q_{ID} = H_2(ID)$, where ID is the signer's identity, and the private key S_{ID} is described by $S_{ID} = sQ_{ID}$ (Page 315, section 3.2, lines 12-17; Page 316, lines 10-11), and

wherein the commitment U is described by $U = r. Q_{ID}$, where r is a random number the signer chooses (Page 316, lines 28-29).

Claim 7

Zhang and Kim disclose the apparatus of claim 6, wherein the blinded message h is described by $h=\alpha^{-1}H_1(m, U')+\beta$, where m is a message to be sent, U' is described by $U'=\alpha U+ \alpha \beta Q_{ID}$ and α and β are blinding factors belonging to Z_q^* (Page 316, lines 28-32).

Claim 8

Zhang and Kim disclose the apparatus of claim 7, wherein the signed message is described by $V=(r+h)S_{ID}$ (Page 316, line 33).

Claim 9

Zhang and Kim disclose the apparatus of claim 8, wherein the means for unblinding is performed by using formula $V'=\alpha V$ (Page 316, line 34).

Claim 10

Zhang and Kim disclose the apparatus of claim 9, wherein the means for verifying is preformed by using following equations: $e(V',P)=e(U',+H_1(m,U')Q_{ID},P_{pub})$ (Page 317, line 3, lines 9-15).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims

are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1 and 6 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-3 and 8-10 of copending application 10747188 (Publication No: US20050005126). Although the conflicting claims are not identical, they are not patentably distinct from each other because for the following reasons.

For claim 1, the Examiner gives a broad interpretation of a method for generating and verifying an ID-based blind signature using bilinear pairings. A ID-based proxy signature includes a ID-based blind signature.

Claim 1 maps to claim 1, 2, and 3 of copending application.

The system parameters include G_1, G_2, e, q, P, P_{pub}, H_1 and H_2, where G_1 is a cyclic additive group whose order is a prime q, G_2 is a cyclic multiplicative group of the same

order q, e is a bilinear paring defined by e: $G_1xG_1 \rightarrow G_2$, P is a generator of G_1, P_{pub} is a trust authority's public key having relationship of $P_{pub}=s.P$, where s is the master key, and H_1 and H_2 are hash functions, respectively, described by H_1: $\{0,1\}^* \rightarrow Z_q^*$ and H_2: $\{0,1\}^* \rightarrow G_1$, where Z_q^* is a cyclic multiplicative group.

The public key Q_{ID} is described by $Q_{ID} = H_2(ID)$, where ID is the signer's identity, and the private key S_{ID} is described by $S_{ID} = sQ_{ID}$. ($Q_A = H_2(A)$, $S_A = sQ_A$) and ($Q_B = H_2(B)$, $S_B = sQ_B$) are equivalent to ($Q_{ID} = H_2(ID)$, $S_{ID} = sQ_{ID}$).

Claim 6 maps to claim 8, 9, and 10 of copending application.

The system parameters include G_1, G_2, e, q, P, P_{pub}, H_1 and H_2, where G_1 is a cyclic additive group whose order is a prime q, G_2 is a cyclic multiplicative group of the same order q, e is a bilinear paring defined by e: $G_1xG_1 \rightarrow G_2$, P is a generator of G_1, P_{pub} is a trust authority's public key having relationship of $P_{pub}=s.P$, where s is the master key, and H_1 and H_2 are hash functions, respectively, described by H_1: $\{0,1\}^* \rightarrow Z_q^*$ and H_2: $\{0,1\}^* \rightarrow G_1$, where Z_q^* is a cyclic multiplicative group.

The public key Q_{ID} is described by $Q_{ID} = H_2(ID)$, where ID is the signer's identity, and the private key S_{ID} is described by $S_{ID} = sQ_{ID}$. ($Q_A = H_2(A)$, $S_A = sQ_A$) and ($Q_B = H_2(B)$, $S_B = sQ_B$) are equivalent to ($Q_{ID} = H_2(ID)$, $S_{ID} = sQ_{ID}$).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Conclusion

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure. The Zhang et al. (Pub. No.: US 20040123110 A1) disclose an apparatus and method for ID-based ring structure by using bilinear pairings. The Boneh et al. (Patent Number: 7,113,594 B2) disclose systems and methods for identity-based encryption and related cryptographic techniques. The Chaum (Patent Number: 4,759,063) discloses blind signature systems. The Zhang, Safavi-Naini, and Lin disclose a new proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairings.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Griffin can be reached on 571-272-1447. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Walter D. Griffin

WALTER D. GRIFFIN
SUPERVISORY PATENT EXAMINER

Canh Le

December 1st, 2006